ESET CYBER SECURITY

para Mac

Manual de instalação e Guia do usuário

Clique aqui para baixar a versão mais recente deste documento



ESET **CYBER SECURITY**

Atendimento ao cliente: www.eset.com/support

REV. 11. 1. 2013

Índice

1. ESET Cyber Security

O ESET Cyber Security representa uma nova abordagem para a segurança do computador verdadeiramente integrada. A versão mais recente do mecanismo de rastreamento do ThreatSense® utiliza velocidade e precisão para manter a segurança do seu computador. O resultado é um sistema inteligente que está constantemente em alerta contra ataques e programas maliciosos que podem comprometer o funcionamento do computador.

O ESET Cyber Security é uma solução de segurança completa desenvolvida a partir do nosso esforço de longo prazo para combinar proteção máxima e impacto mínimo no sistema. As tecnologias avançadas, com base em inteligência artificial, são capazes de eliminar proativamente a infiltração por vírus, spywares, cavalos de troia, worms, adwares, rootkits e outros ataques via Internet sem prejudicar o desempenho do sistema ou interromper a atividade do computador.

1.1 Novidades

Proteção de cliente de email
A proteção de email fornece controle da comunicação por email recebida via protocolos POP3 e IMAP.

Rastreamento de mídia removível
O ESET Cyber Security oferece um rastreamento sob demanda do dispositivo de mídia removível inserido (CD, DVD, USB, dispositivo iOS, etc.).

Ingresse na rede ESET Live Grid
Criado a partir do sistema de alerta antecipado avançado ThreatSense.NET, o ESET Live Grid foi projetado para fornecer níveis adicionais de segurança a seu computador. Ele monitora constantemente os programas em execução no sistema e processa com relação à inteligência mais recente coletada de milhões de usuários do ESET em todo o mundo. Adicionalmente, os rastreamentos do sistema são processados mais rápida e precisamente à medida que o banco de dados do ESET Live Grid cresce no decorrer do tempo. Isto nos permite oferecer proteção proativa e velocidade de rastreamento cada vez maiores para todos os nossos usuários. Recomendamos que você ative esse recurso e agradecemos pelo seu suporte.

Novo design
A janela principal do ESET Cyber Security recebeu um novo design completo e a Configuração avançada está mais intuitiva para facilitar a navegação.

1.2 Requisitos do sistema

Para uma operação ideal do ESET Cyber Security, seu sistema deve atender aos seguintes requisitos de hardware e de software:

	Requisitos do sistema
Arquitetura do processador	32 bits, 64 bits Intel®
Sistema operacional	Mac OS X 10.6 e posterior
Memória	300 MB
Espaço livre em disco	150 MB

2. Instalação

Antes de iniciar o processo de instalação, feche todos os programas abertos no computador. O ESET Cyber Security contém componentes que podem entrar em conflito com outros programas antivírus que já podem estar instalados no computador. A ESET recomenda veementemente remover qualquer outro programa antivírus para evitar problemas potenciais.

Para iniciar o assistente de instalação, execute uma das seguintes ações:

- Se você estiver instalando a partir de um CD/DVD de instalação, insira-o no computador, abra-o em sua área de trabalho ou na janela do **Finder** e clique duas vezes no ícone **Instalar**.
- Se estiver instalando de um arquivo obtido do site da ESET, abra o arquivo e clique duas vezes no ícone **Instalar**.



Inicie o instalador e o assistente de instalação o guiará pela configuração básica. Durante a fase inicial da instalação, o instalador verificará automaticamente on-line se há uma versão mais recente do produto. Se encontrada, o instalador a oferecerá para download e iniciará o processo de instalação.

Após concordar com o Contrato de licença de usuário final, você poderá escolher um dos seguintes modos de instalação:

- Instalação típica 4
- Instalação personalizada 5

2.1 Instalação típica

O modo de instalação típica inclui opções de configuração apropriadas para a maioria dos usuários. Essas configurações proporcionam segurança máxima combinada com o excelente desempenho do sistema. A instalação típica é a opção padrão e é recomendada se você não possui requisitos particulares para configurações específicas.

Live Grid
O Live Grid Early Warning System é a melhor maneira de você ajudar a ESET a estar, imediatamente e continuamente, informada sobre novas infiltrações, a fim de proteger

rapidamente nossos clientes. O sistema permite o envio de novas ameaças para o Laboratório de ameaças da ESET, onde serão analisadas, processadas e adicionadas ao banco de dados de assinatura de vírus. Por padrão, a opção **Ativar Live Grid Early Warning System** está selecionada. Clique em **Configurar...** para modificar as configurações detalhadas sobre o envio de arquivos suspeitos. Para obter mais informações, consulte Live Grid 18.

Aplicativos especiais
A última etapa do processo de instalação é a configuração da detecção de **Aplicativos potencialmente não desejados**. Esses programas não são necessariamente maliciosos, mas podem prejudicar o comportamento do sistema operacional. Esses aplicativos são frequentemente vinculados a outros programas e podem ser difíceis de notar durante o processo de instalação. Embora esses aplicativos geralmente exibam uma notificação durante a instalação, eles podem ser instalados facilmente sem o seu consentimento.

Após instalar o ESET Cyber Security, você deve executar um rastreamento do computador para verificar se há código malicioso. Na janela principal do programa, clique em **Rastrear o computador** e, em seguida, em **Rastreamento inteligente**. Para obter mais informações sobre os rastreamentos sob demanda do computador, consulte a seção Rastreamento sob demanda do computador 8.

2.2 Instalação personalizada

O modo de instalação personalizada é destinado a usuários experientes que desejam modificar as configurações avançadas durante o processo de instalação.

Servidor proxy
Se estiver utilizando um servidor proxy, você poderá definir os parâmetros agora, selecionando a opção **Eu utilizo um servidor proxy**. Na próxima etapa, digite o endereço IP ou o URL do seu servidor proxy no campo **Endereço**. No campo **Porta**, especifique a porta em que o servidor proxy aceita as conexões (3128 por padrão). Caso o servidor proxy exija autenticação, digite um **usuário** e uma **senha** válidos a fim de obter acesso ao servidor proxy. Se tiver certeza de que nenhum servidor proxy está sendo utilizado, escolha a opção **Eu não utilizo um servidor proxy**. Se não tiver certeza, você poderá utilizar as configurações atuais do sistema, selecionando **Usar as configurações do sistema (Recomendável)**.

Privilégios
Na próxima etapa, você poderá definir usuários privilegiados que poderão editar a configuração do programa. Em uma lista de usuários, no lado esquerdo, selecione os usuários e selecione **Adicionar** para incluí-los na lista **Usuários privilegiados**. Para exibir todos os usuários do sistema, selecione a opção **Mostrar todos os usuários**. Se você deixar a lista Usuários privilegiados vazio, todos os usuários serão considerados privilegiados.

Live Grid
O Live Grid Early Warning System é a melhor maneira de você ajudar a ESET a estar, imediatamente e continuamente, informada sobre novas infiltrações, a fim de proteger

rapidamente nossos clientes. O sistema permite o envio de novas ameaças para o Laboratório de ameaças da ESET, onde serão analisadas, processadas e adicionadas ao banco de dados de assinatura de vírus. Por padrão, a opção **Ativar Live Grid Early Warning System** está selecionada. Clique em **Configurar...** para modificar as configurações detalhadas sobre o envio de arquivos suspeitos. Para obter mais informações, consulte Live Grid 18.

Aplicativos especiais
A próxima etapa do processo de instalação é a configuração da detecção de **Aplicativos potencialmente não desejados**. Esses programas não são necessariamente maliciosos, mas podem prejudicar o comportamento do sistema operacional. Esses aplicativos são frequentemente vinculados a outros programas e podem ser difíceis de notar durante o processo de instalação. Embora esses aplicativos geralmente exibam uma notificação durante a instalação, eles podem ser instalados facilmente sem o seu consentimento.

Após instalar o ESET Cyber Security, você deve executar um rastreamento do computador para verificar se há código malicioso. Na janela principal do programa, clique em **Rastrear o computador** e, em seguida, em **Rastreamento inteligente**. Para obter mais informações sobre os rastreamentos sob demanda do computador, consulte a seção Rastreamento sob demanda do computador 8.

3. Ativação do produto

Depois da instalação, a janela **Tipo de ativação do produto** será exibida automaticamente em sua tela. Como alternativa, é possível clicar no ícone do ESET Cyber Security, localizado na barra de menus (topo da tela), e clicar em **Ativação do produto...**.

1. Se você adquiriu uma versão do produto em um caixa no varejo, selecione a opção **Ativar usando uma Chave de ativação**. A Chave de ativação está normalmente localizada no interior ou na parte posterior da embalagem do produto. Para uma ativação bem sucedida, a Chave de ativação deve ser digitada conforme fornecida.

2. Se você recebeu um Usuário e uma Senha, selecione a opção **Ativar utilizando um Usuário e Senha** e digite os dados da licença nos campos apropriados. Essa opção é equivalente à opção **Configuração do usuário e senha...** na janela **Atualizar** do programa.

3. Se desejar avaliar o ESET Cyber Security antes de fazer uma aquisição, selecione a opção **Ativar licença de avaliação**. Preencha o seu endereço de email para ativar a versão de avaliação do ESET Cyber Security por um período limitado. A licença de teste será enviada para seu email. A licença de avaliação pode ser ativada apenas uma vez por cliente.

Se você escolher não ativar agora, clique em **Ativar mais tarde**. Você pode ativar o ESET Cyber Security diretamente da seção **Início** ou **Atualizar** da janela principal do programa ESET Cyber Security.

Se você não tem uma licença e deseja adquirir uma, clique na opção **Licença**. Isso o redirecionará para o site do seu distribuidor local da ESET.

4. Desinstalação

Se você desejar desinstalar o ESET Cyber Security do seu computador, execute uma das seguintes ações:

- insira o CD/DVD de instalação do ESET Cyber Security em seu computador, abra-o em sua área de trabalho ou na janela do **Finder** e clique duas vezes no ícone **Desinstalar**.
- abra o arquivo de instalação do ESET Cyber Security (*.dmg*) e clique duas vezes no ícone **Desinstalar**,
- inicie o **Finder**, abra a pasta **Aplicativos** na sua unidade de disco rígido, pressione Ctrl e clique no ícone do **ESET Cyber Security** e selecione a opção **Mostrar conteúdos do pacote**. Abra a pasta **Recursos** e clique duas vezes no ícone **Desinstalar**.

5. Visão geral básica

A janela principal do ESET Cyber Security é dividida em duas seções principais. A janela principal à direita exibe informações correspondentes à opção selecionada no menu principal à esquerda.

A seguir, há uma descrição das opções dentro do menu principal:

- **Início** - fornece informações sobre o status da proteção de sua proteção de email, web e computador.
- **Rastrear o computador** - esta opção permite configurar e iniciar o rastreamento Sob Demanda do computador 8.
- **Atualizar** - exibe informações sobre as atualizações do banco de dados de assinatura de vírus.
- **Configurar** - selecione esta opção para ajustar o nível de segurança do seu computador.
- **Ferramentas** - fornece acesso a arquivos de log 15, agenda 16, quarentena 17, processos em execução 17 e outros recursos do programa.
- **Ajuda** - exibe acesso a arquivos de ajuda, base de dados de conhecimento da Internet, formulário de solicitação de suporte e informações adicionais sobre o programa.

5.1 Teclas de atalho do teclado

As teclas de atalho que podem ser usadas ao trabalhar com o ESET Cyber Security incluem:

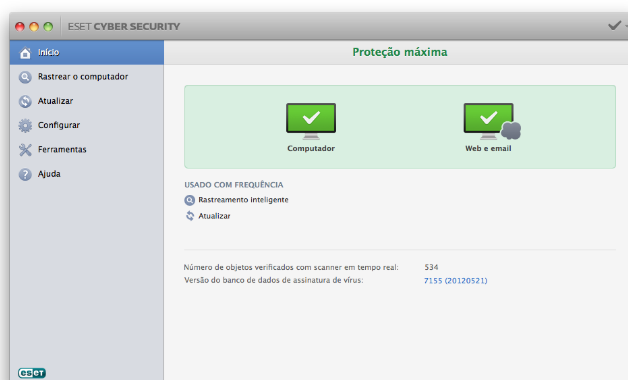
- *cmd-,* - exibe as Preferências do ESET Cyber Security,
- *cmd-U* - abre a janela **Configuração do usuário e senha**,
- *cmd-alt-T* - abre a janela **Caracteres especiais**,
- *cmd-O* - redimensiona a janela de interface gráfica do usuário principal do ESET Cyber Security para o tamanho padrão e a move para o centro da tela,
- *cmd-alt-H* - oculta todas as janelas abertas, exceto o ESET Cyber Security,
- *cmd-H* - oculta o ESET Cyber Security.

As seguintes teclas de atalho do teclado funcionarão somente se a opção **Usar menu padrão** estiver habilitada em **Configuração > Entrar nas preferências do aplicativo...** (ou pressione *cmd-,*) > **Interface**:

- *cmd-alt-L* - abre a seção **Arquivos de log**,
- *cmd-alt-S* - abre a seção **Agenda**,
- *cmd-alt-Q* - abre a seção **Quarentena**.

5.2 Verificação do funcionamento do programa

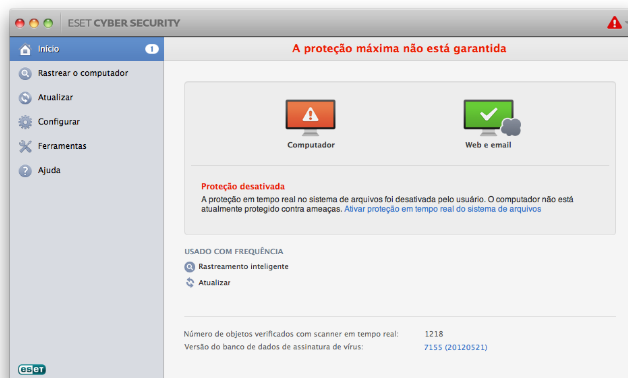
Para ver o status da proteção, clique na opção **Início** do menu principal. Um resumo de status sobre o funcionamento dos módulos do ESET Cyber Security será exibido na janela principal.



5.3 O que fazer se o programa não funcionar adequadamente

Se os módulos ativados estiverem funcionando adequadamente, um ícone verde será atribuído a eles. Caso contrário, um ponto de exclamação vermelho ou um ícone de notificação laranja será exibido, e informações adicionais sobre o módulo e uma solução sugerida para corrigir o problema serão mostradas. Para alterar o status dos módulos individuais, clique no link azul abaixo de cada mensagem de notificação.

Se não for possível solucionar um problema com as soluções sugeridas, você poderá pesquisar uma solução na Base de dados de conhecimento da ESET ou entrar em contato com o Atendimento ao cliente da ESET. O Atendimento ao cliente responderá rapidamente às suas dúvidas e o ajudará a determinar uma resolução.



6. Proteção do computador

A configuração do computador pode ser encontrada em **Configurar** > **Computador**. Ela mostrará o status de **Proteção em tempo real do sistema de arquivos** e **Bloquear mídia removível**. Para desativar módulos individuais, alterne o botão do módulo desejado para **DESATIVADO**. Observe que essa ação pode diminuir a proteção do seu computador. Para acessar as configurações detalhadas de cada módulo, clique no botão **Configurar...**.

6.1 Proteção antivírus e antispyware

A proteção antivírus protege contra ataques de sistemas maliciosos, modificando arquivos que representam ameaças internas. Se uma ameaça com código malicioso for detectada, o módulo antivírus poderá eliminá-la, bloqueando-a e, em seguida, limpando, excluindo ou movendo-a para a quarentena.

6.1.1 Proteção em tempo real do sistema de arquivos

A proteção do sistema de arquivos em tempo real verifica todos os tipos de mídia e aciona um rastreamento com base em vários eventos. Usando os métodos de detecção da tecnologia ThreatSense (descritos na seção intitulada Configuração de parâmetros do mecanismo ThreatSense 10), a proteção do sistema de arquivos em tempo real pode variar para arquivos recém-criados e existentes. Em arquivos recém-criados, é possível aplicar um nível mais profundo de controle.

Por padrão, a proteção em tempo real é ativada no momento da inicialização do sistema, proporcionando rastreamento ininterrupto. Em casos especiais (por exemplo, se houver um conflito com outro rastreador em tempo real), a proteção em tempo real pode ser terminada, clicando no ícone do ESET Cyber Security, localizado na barra de menus (topo da tela), e selecionando a opção **Desativar a proteção em tempo real do sistema de arquivos**. A proteção em tempo real também pode ser terminada na janela principal do programa (clique em **Configurar** > **Computador** e alterne **Proteção em tempo real do sistema de arquivos** para **DESATIVADO**).

Para modificar as configurações avançadas da proteção em tempo real, vá para **Configuração** > **Entrar nas preferências do aplicativo...** (ou pressione *cmd-,*) > **Proteção em tempo real** e clique no botão **Configurar...**, próximo das **Opções avançadas** (descritas na seção denominada Opções de rastreamento avançadas 7).

6.1.1.1 Rastreamento ativado (Rastreamento disparado por evento)

Por padrão, todos os arquivos são rastreados na abertura, criação ou execução do arquivo. Recomendamos que você mantenha as configurações padrão, uma vez que elas fornecem o nível máximo de proteção em tempo real ao seu computador.

6.1.1.2 Opções avançadas

Nessa janela, é possível definir os tipos de objeto que serão rastreados pelo mecanismo ThreatSense, e ativar/desativar **Heurística avançada** e também modificar as configurações de arquivos compactados e cache de arquivo.

Não recomendamos alterar os valores padrão na seção **Configurações padrão de arquivos compactados**, a menos que seja necessário resolver um problema específico, pois os valores maiores de compactação de arquivos compactados podem impedir o desempenho do sistema.

Você pode alternar o rastreamento da Heurística avançada ThreatSense para arquivos executados, criados e modificados separadamente, clicando na caixa de seleção **Heurística avançada** em cada uma das respectivas seções de parâmetros do ThreatSense .

Para proporcionar o impacto mínimo no sistema ao usar a proteção em tempo real, você pode definir o tamanho do cache de otimização. Esse comportamento fica ativo durante a utilização da opção **Ativar cache de arquivo limpo**. Se esse recurso for desativado, todos os arquivos serão rastreados toda vez que forem acessados. Os arquivos não serão rastreados repetidamente após serem ocultados (a menos que sejam modificados), até o tamanho definido do cache. Os arquivos são rastreados novamente logo após cada atualização do banco de dados de assinatura de vírus. Clique em **Ativar cache de arquivo limpo** para ativar/desativar essa função. Para definir a quantidade de arquivos que serão ocultados, basta digitar o valor desejado no campo de entrada, ao lado de **Tamanho do cache**.

Os parâmetros de rastreamento adicionais podem ser configurados na janela **Configuração do mecanismo ThreatSense**. Você pode definir os tipos de **Objetos** que devem ser rastreados, utilizando o nível **Opções** e **Limpeza** e também definindo **Extensões** e **Limites** de tamanho de arquivos para a proteção em tempo real do sistema de arquivos. Você pode inserir a janela de configuração do mecanismo ThreatSense clicando no botão **Configurar...** ao lado de **Mecanismo ThreatSense**, na janela Configuração avançada. Para obter informações mais detalhadas sobre os parâmetros do mecanismo ThreatSense, consulte Configuração de parâmetros do mecanismo ThreatSense 10.

6.1.1.3 Quando modificar a configuração da proteção em tempo real

A proteção em tempo real é o componente mais essencial para a manutenção de um sistema seguro. Tenha cautela ao modificar os parâmetros da proteção em tempo real. Recomendamos que você modifique esses parâmetros apenas em casos específicos. Por exemplo, se houver uma situação de conflito com um certo aplicativo ou rastreador em tempo real de outro programa antivírus.

Após instalar o ESET Cyber Security, todas as configurações serão otimizadas para proporcionar o nível máximo de segurança do sistema para os usuários. Para restaurar as configurações padrão, clique no botão **Padrão** localizado na parte inferior esquerda da janela **Proteção em tempo real** (**Configurar** > **Entrar nas preferências do aplicativo ...** > **Proteção em tempo real**).

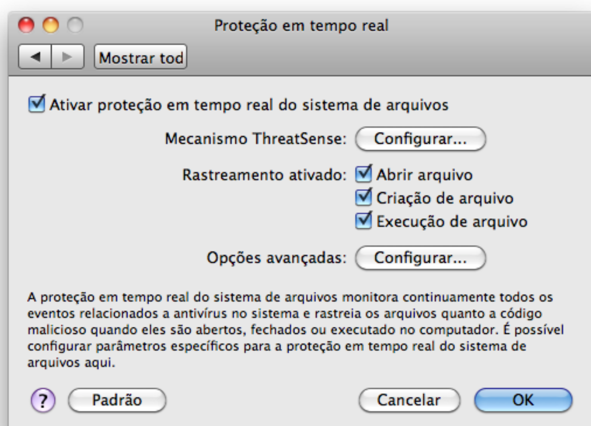
6.1.1.4 Verificação da proteção em tempo real

Para verificar se a proteção em tempo real está funcionando e detectando vírus, utilize o arquivo de teste eicar.com. Esse arquivo de teste é especial, inofensivo e detectável por todos os programas antivírus. O arquivo foi criado pelo instituto EICAR (European Institute for Computer Antivirus Research) para testar a funcionalidade de programas antivírus.

6.1.1.5 O que fazer se a proteção em tempo real não funcionar

Neste capítulo, descrevemos situações problemáticas que podem surgir quando usamos proteção em tempo real e como solucioná-las.

Proteção em tempo real desativada
Se a proteção em tempo real foi inadvertidamente desativada por um usuário, será preciso reativá-la. Para reativar a Proteção em tempo real, navegue até **Configurar** > **Computador** e alterne **Proteção em tempo real do sistema de arquivos** para **ATIVADO**. Como alternativa, você pode ativar a proteção em tempo real do sistema de arquivos na janela de preferências do aplicativo, em **Proteção em tempo real**, selecionando a opção **Ativar proteção em tempo real do sistema de arquivos**.



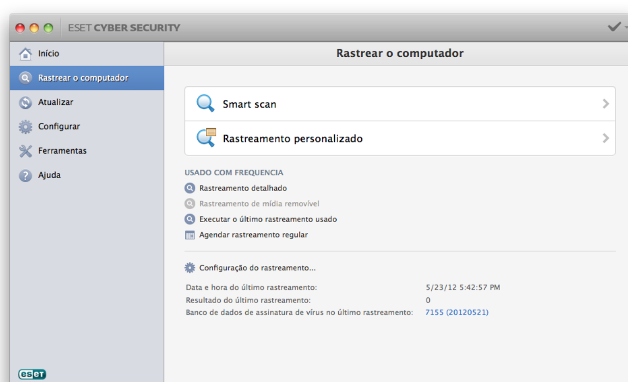
Proteção em tempo real não detecta nem limpa infiltrações
Verifique se não há algum outro programa antivírus instalado no computador. Se duas proteções em tempo real forem ativadas ao mesmo tempo, elas poderão entrar em conflito. Recomendamos desinstalar outros programas antivírus que possam estar no sistema.

A proteção em tempo real não é iniciada
Se a proteção em tempo real não for ativada na inicialização do sistema, talvez haja conflitos com outros programas. Se for este o caso, consulte os especialistas do Atendimento ao Cliente da ESET.

6.1.2 Rastreamento sob demanda do computador

Caso suspeite que seu computador esteja infectado (se ele se comportar de maneira anormal), execute **Rastreamento do computador** > **Rastreamento inteligente** para examinar se há infiltrações no computador. Para obter proteção máxima, os rastreamentos do computador devem ser executados regularmente como parte das medidas usuais de segurança; não faça rastreamentos somente sob suspeita de infecção. O rastreamento normal pode detectar infiltrações que não foram detectadas pelo rastreador em tempo real quando foram salvas no disco. Isso pode acontecer caso o rastreador em tempo real esteja desativado no momento da infecção ou se o banco de dados de assinatura de vírus não estiver atualizado.

Recomendamos que execute um Rastreamento sob demanda do computador pelo menos uma vez por mês. O rastreamento pode ser configurado como uma tarefa agendada em **Ferramentas** > **Agenda**.



Você também pode arrastar e soltar pastas e arquivos da sua área de trabalho ou da janela **Finder** para a tela principal do ESET Cyber Security, para o ícone de âncora, ícone da barra de menu (parte superior da tela) ou para o ícone do aplicativo (localizado na pasta */Aplicativos*).

6.1.2.1 Tipos de rastreamento

Há dois tipos de rastreamento sob demanda do computador disponíveis. O **Rastreamento inteligente** rastreia rapidamente o sistema sem necessidade de mais configurações dos parâmetros de rastreamento. O **Rastreamento personalizado** permite selecionar qualquer perfil de rastreamento predefinido e também permite escolher alvos de rastreamento específicos.

6.1.2.1.1 Rastreamento inteligente

O Rastreamento inteligente permite que você inicie rapidamente um rastreamento do computador e limpe arquivos infectados, sem a necessidade de intervenção do usuário. Sua principal vantagem é a operação fácil, sem configurações de rastreamento detalhadas. O Rastreamento inteligente verifica todos os arquivos em todas as pastas e limpa ou exclui automaticamente as infiltrações detectadas. O nível de limpeza é automaticamente ajustado ao valor padrão. Para obter informações mais detalhadas sobre os tipos de limpeza, consulte a seção sobre Limpeza 11.

6.1.2.1.2 Rastreamento personalizado

O **Rastreamento personalizado** é excelente caso deseje especificar parâmetros de rastreamento, como alvos de rastreamento e métodos de rastreamento. A vantagem de executar o Rastreamento personalizado é a capacidade de configurar os parâmetros detalhadamente. Diferentes configurações podem ser salvas nos perfis de rastreamento definidos pelo usuário, o que poderá ser útil se o rastreamento for executado repetidas vezes com os mesmos parâmetros.

Para selecionar os alvos de rastreamento, selecione **Rastrear o computador** > **Rastreamento personalizado** e selecione **Alvos de rastreamento** na estrutura em árvore. Um alvo de rastreamento pode ser também mais exatamente especificado por meio da inserção do caminho para a pasta ou arquivo(s) que você deseja incluir. Se você estiver interessado apenas no rastreamento do sistema, sem ações de limpeza adicionais, selecione a opção **Rastrear sem limpar**. Além disso, você pode selecionar entre três níveis de limpeza clicando em **Configurar...** > **Limpeza**.

OBSERVAÇÃO: A realização de rastreamentos de computador com o Rastreamento personalizado é recomendada para usuários avançados com experiência anterior na utilização de programas antivírus.

6.1.2.2 Alvos de rastreamento

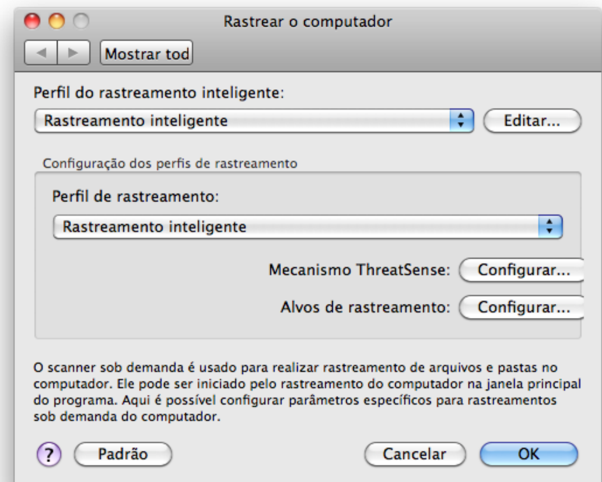
A estrutura em árvore de Alvos de rastreamento permite que você selecione arquivos e pastas que serão rastreados em busca de vírus. As pastas também podem ser selecionadas de acordo com as configurações de um perfil.

Um alvo de rastreamento pode ser mais exatamente definido por meio da inserção do caminho para a pasta ou arquivo(s) que você deseja incluir no rastreamento. Selecione alvos na estrutura em árvore que lista todas as pastas disponíveis no computador.

6.1.2.3 Perfis de rastreamento

As suas configurações de rastreamento favoritas podem ser salvas para rastreamento futuro. Recomendamos a criação de um perfil diferente (com diversos alvos de rastreamento, métodos de rastreamento e outros parâmetros) para cada rastreamento utilizado regularmente.

Para criar um novo perfil, vá para **Configurar** > **Entrar nas preferências do aplicativo ...** (ou pressione *cmd-,*) > **Rastrear o computador** e clique em **Editar...** ao lado da lista de perfis atuais.



Para ajudar a criar um perfil de rastreamento a fim de atender às suas necessidades, consulte a seção Configuração de parâmetros do mecanismo ThreatSense 10 para obter uma descrição de cada parâmetro da configuração de rastreamento.

Exemplo: Suponhamos que você deseje criar seu próprio perfil de rastreamento e que a configuração de Rastreamento inteligente seja parcialmente adequada. Porém, você não deseja rastrear empacotadores em tempo real nem aplicativos potencialmente inseguros e também deseja aplicar a Limpeza rígida. Na janela **Lista de perfis do scanner sob demanda**, digite o nome do perfil, clique no botão **Adicionar** e confirme clicando em **OK**. Ajuste os parâmetros que atendam aos seus requisitos, configurando o **Mecanismo ThreatSense** e **Alvos de rastreamento**.

6.1.3 Exclusões

Esta seção (**Configurar** > **Entrar nas preferências do aplicativo...** > **Exclusões**) permite que você exclua determinados arquivos/pastas, aplicativos ou endereços IP/IPv6 do rastreamento.

Arquivos e pastas relacionados na lista **Sistema de arquivos** serão excluídos de todos os scanners: Sistema (inicialização), Em tempo real e Sob demanda.

- **Caminho** – caminho para arquivos e pastas excluídos
- **Ameaça** - se houver um nome de uma ameaça próximo a um arquivo excluído, significa que o arquivo só foi excluído para a determinada ameaça, e não completamente. Portanto, se o arquivo for infectado posteriormente com outro malware, ele será detectado pelo módulo antivírus.
- **Adicionar...** - exclui objetos da detecção. Insira o caminho para um objeto (você também pode utilizar caracteres curinga *** e *?*) ou selecione a pasta ou o arquivo na estrutura em árvore.

- **Editar...** - permite que você edite as entradas selecionadas
- **Excluir** - remove as entradas selecionadas.
- **Padrão** – cancela todas as exclusões.

Na guia **Web e email**, você pode excluir determinados **Aplicativos** ou **Endereços IP/IPv6** do rastreamento de protocolos.

6.1.4 Configuração de parâmetros do mecanismo ThreatSense

O ThreatSense é uma tecnologia proprietária da ESET que consiste de uma combinação de métodos complexos de detecção de ameaças. Essa tecnologia é proativa, o que significa que ela também fornece proteção durante as primeiras horas da propagação de uma nova ameaça. Ela utiliza uma combinação de diversos métodos (análise de código, emulação de código, assinaturas genéricas e assinaturas de vírus) que funcionam em conjunto para otimizar significativamente a segurança do sistema. O mecanismo de rastreamento é capaz de controlar diversos fluxos de dados simultaneamente, maximizando a eficiência e a taxa de detecção. A tecnologia ThreatSense também evita com êxito os rootkits.

As opções de configuração da tecnologia ThreatSense permitem que você especifique diversos parâmetros de rastreamento:

- Tipos e extensões de arquivos que serão rastreados
- A combinação de diversos métodos de detecção
- Níveis de limpeza etc.

Para entrar na janela de configuração, clique em **Configurar > Entrar nas preferências do aplicativo...** (ou pressione `cmd-,`) e clique no botão Mecanismo ThreatSense **Configurar...**, localizado nos caracteres curinga **Proteção do sistema**, **Proteção em tempo real** e **Rastrear o computador** todos os quais usam a tecnologia ThreatSense (veja a seguir). Cenários de segurança diferentes podem exigir configurações diferentes. Com isso em mente, o ThreatSense é configurado individualmente para os seguintes módulos de proteção:

- **Proteção do sistema** - Rastreamento de arquivo na inicialização do sistema
- **Proteção em tempo real** - Proteção em tempo real do sistema de arquivos
- **Rastrear o computador** - Rastreamento sob demanda do computador

Os parâmetros do ThreatSense são especificamente otimizados para cada módulo e a modificação deles pode influenciar significativamente o funcionamento do sistema. Por exemplo, a alteração das configurações para sempre rastrear empacotadores em tempo real ou a ativação da heurística avançada no módulo de proteção em tempo real de sistema de arquivos podem resultar em um sistema mais lento. Portanto, recomendamos que mantenha os parâmetros padrão do ThreatSense inalterados para todos os módulos, exceto o Rastrear o computador.

6.1.4.1 Objetos

A seção **Objetos** permite definir quais arquivos do computador serão rastreados quanto a infiltrações.

- **Arquivos** - fornece o rastreamento de todos os tipos de arquivos comuns (programas, imagens, áudio, arquivos de vídeo, arquivos de banco de dados etc.)
- **Links simbólicos** - (somente scanner sob demanda) rastreia determinados tipos especiais de arquivos que contenham uma cadeia de caracteres de texto que seja interpretada e seguida pelo sistema operacional como um caminho para outro arquivo ou diretório.
- **Arquivos de email** - (não disponível na Proteção em tempo real) rastreia arquivos especiais que contenham mensagens de e-mail.
- **Caixas de correio** - (não disponível na Proteção em tempo real) rastreia as caixas de correio do usuário no sistema. A utilização incorreta dessa opção pode resultar em um conflito com o seu cliente de e-mail. Para saber mais sobre as vantagens e desvantagens dessa opção, leia o seguinte artigo da base de dados de conhecimento.
- **Arquivos compactados** - (não disponível na proteção em tempo real) fornece o rastreamento de arquivos compactados (.rar, .zip, .arj, .tar etc.).
- **Arquivos compactados de auto-extração** - (não disponível na Proteção em tempo real) rastreia arquivos contidos em arquivos compactados de auto-extração.
- **Empacotadores em tempo real** - diferente dos tipos de arquivos compactados padrão, os empacotadores em tempo real são descompactados na memória, além de empacotadores estáticos padrão (UPX, yoda, ASPack, FGS etc.).

6.1.4.2 Opções

Na seção **Opções**, você pode selecionar os métodos utilizados durante um rastreamento do sistema para verificar infiltrações. As seguintes opções estão disponíveis:

- **Heurística** - A heurística utiliza um algoritmo que analisa a atividade (maliciosa) de programas. A principal vantagem da detecção heurística é a capacidade de detectar novos softwares maliciosos, que não existiam antes ou não estavam incluídos na lista de vírus conhecidos (banco de dados de assinatura de vírus).
- **Heurística avançada** - A heurística avançada é constituída por um algoritmo heurístico exclusivo, desenvolvido pela ESET, otimizado para a detecção de worms e cavalos de troia de computador escritos em linguagens de programação de alto nível. A capacidade de detecção do programa é significativamente maior por causa da heurística avançada.

- **Aplicativos potencialmente indesejados** - Esses aplicativos não são necessariamente maliciosos, mas podem afetar o desempenho do seu computador de maneira negativa. Tais aplicativos geralmente exigem o consentimento para a instalação. Se eles estiverem presentes em seu computador, o seu sistema se comportará de modo diferente (em comparação ao modo anterior à instalação desses aplicativos). As alterações mais significativas são janelas pop-up indesejadas, ativação e execução de processos ocultos, aumento do uso de recursos do sistema, modificações nos resultados de pesquisa e aplicativos se comunicando com servidores remotos.
- **Aplicativos potencialmente inseguros** - esses aplicativos referem-se a softwares comerciais e legítimos que podem sofrer abusos por parte de invasores, caso tenham sido instalados sem o conhecimento do usuário. Essa classificação inclui programas como ferramentas de acesso remoto, motivo pelo qual essa opção, por padrão, é desativada.

6.1.4.3 Limpeza

As configurações de limpeza determinam como o scanner limpa os arquivos infectados. Há três níveis de limpeza:

- **Sem limpeza** - Os arquivos infectados não são limpos automaticamente. O programa exibirá uma janela de aviso e permitirá que você escolha uma ação.
- **Limpeza padrão** - O programa tentará limpar ou excluir automaticamente um arquivo infectado. Se não for possível selecionar a ação correta automaticamente, o programa oferecerá uma escolha de ações a serem seguidas. A escolha das ações a serem seguidas também será exibida se uma ação predefinida não for completada.
- **Limpeza rígida** – O programa limpará ou excluirá todos os arquivos infectados (incluindo os arquivos compactados). As únicas exceções são os arquivos do sistema. Se não for possível limpá-los, será oferecida a você uma ação a ser tomada na janela de aviso.

Aviso: No modo de limpeza Padrão, o arquivo compactado inteiro será excluído somente se todos os arquivos do arquivo compactado estiverem infectados. Se no arquivo compactado houver arquivos legítimos, ele não será excluído. Se um arquivo do arquivo compactado infectado for detectado no modo de Limpeza rígida, todo o arquivo compactado será excluído, mesmo se houver arquivos limpos.

6.1.4.4 Extensões

Uma extensão é a parte do nome de arquivo delimitada por um ponto final. A extensão define o tipo e o conteúdo do arquivo. Esta seção de configuração de parâmetros do ThreatSense permite definir os tipos de arquivos a serem excluídos do rastreamento.

Por padrão, todos os arquivos são rastreados, independentemente de suas extensões. Qualquer extensão pode ser adicionada à lista de arquivos excluídos do rastreamento. Com os botões **Adicionar** e **Remover**, você pode habilitar ou desabilitar o rastreamento das extensões desejadas.

A exclusão de arquivos do rastreamento será necessária algumas vezes se o rastreamento de determinados tipos de arquivos impedir o funcionamento correto do programa. Por exemplo, pode ser aconselhável excluir as extensões *.log*, *.cfg* e *.tmp*.

6.1.4.5 Limites

A seção **Limites** permite especificar o tamanho máximo de objetos e os níveis de compactação de arquivos compactados a serem rastreados:

- **Tamanho máximo:** Define o tamanho máximo dos objetos que serão rastreados. O módulo antivírus rastreará apenas objetos menores que o tamanho especificado. Não recomendamos alterar o valor padrão, pois geralmente não há razão para modificá-lo. Essa opção deverá ser alterada apenas por usuários avançados que tenham razões específicas para excluir objetos maiores do rastreamento.
- **Tempo máximo do rastreamento:** Define o tempo máximo designado para o rastreamento de um objeto. Se um valor definido pelo usuário for digitado aqui, o módulo antivírus interromperá o rastreamento de um objeto quando o tempo tiver decorrido, independentemente da conclusão do rastreamento.
- **Nível de compactação de arquivos:** Especifica a profundidade máxima do rastreamento de arquivos compactados. Não recomendamos alterar o valor padrão de 10; sob circunstâncias normais, não haverá razão para modificá-lo. Se o rastreamento for encerrado prematuramente devido ao número de arquivos compactados aninhados, o arquivo compactado permanecerá desmarcado.
- **Tamanho máximo do arquivo:** Esta opção permite especificar o tamanho máximo de arquivo dos arquivos contidos em arquivos compactados (quando são extraídos) a ser rastreados. Se o rastreamento for encerrado prematuramente por causa desse limite, o arquivo compactado permanecerá sem verificação.

6.1.4.6 Outros

Ativar otimização inteligente
Com a Otimização inteligente ativada, as configurações são otimizadas para garantir o nível mais eficiente de rastreamento, sem comprometer a velocidade de rastreamento. Os diversos módulos de proteção fazem rastreamento de maneira inteligente, utilizando diferentes métodos de rastreamento. Otimização inteligente não é definida rigidamente no produto. A equipe de desenvolvimento da ESET está implementando continuamente as novas alterações que foram integradas ao ESET Cyber Security por meio de atualizações regulares. Se a Otimização inteligente estiver desativada, somente as configurações definidas pelo usuário no núcleo do ThreatSense do módulo particular serão aplicadas durante a realização de um rastreamento.

Rastrear fluxos de dados alternativos (somente scanner sob demanda)
Os fluxos de dados alternativos (bifurcações de recursos/ dados) usados pelo sistema de arquivos são associações de arquivos e pastas invisíveis às técnicas comuns de rastreamento. Muitas infiltrações tentam evitar a detecção disfarçando-se de fluxos de dados alternativos.

6.1.5 Uma infiltração foi detectada

As infiltrações podem atingir o sistema a partir de vários pontos de entrada: páginas da Web, pastas compartilhadas, email ou dispositivos de computador removíveis (USB, discos externos, CDs, DVDs, etc.).

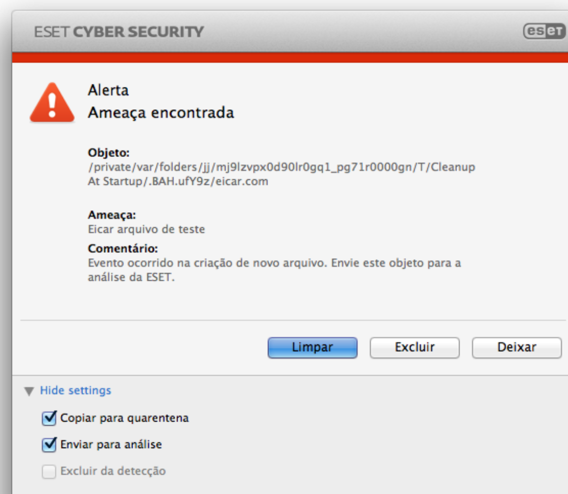
Se o seu computador estiver apresentando sinais de infecção por malware, por exemplo, estiver mais lento, travar com frequência etc., recomendamos as seguintes etapas:

1. Clique em **Rastrear o computador**.
2. Clique em **Rastreamento inteligente** (para obter mais informações, consulte a seção Rastreamento inteligente 8).
3. Após o rastreamento ter terminado, revise o log para obter informações como o número dos arquivos verificados, infectados e limpos.

Se desejar rastrear apenas uma determinada parte do seu disco, clique em **Rastreamento personalizado** e selecione os alvos a serem rastreados quanto a vírus.

Como exemplo geral de como as infiltrações são tratadas no ESET Cyber Security, suponha que uma infiltração seja detectada pelo monitor do sistema de arquivos em tempo real, que usa o nível de limpeza padrão. Ele tentará limpar ou excluir o arquivo. Se não houver uma ação predefinida disponível para o módulo de proteção em tempo real, você será solicitado a selecionar uma opção em uma janela de alertas. Geralmente as opções **Limpar**, **Excluir** e **Nenhuma ação** estão disponíveis. A seleção da opção **Nenhuma ação** não é recomendada, visto que o(s) arquivo(s) infectado(s) é (são) mantido(s) intocado(s). Uma exceção a isso é quando você tem certeza de que o arquivo é inofensivo e foi detectado por engano.

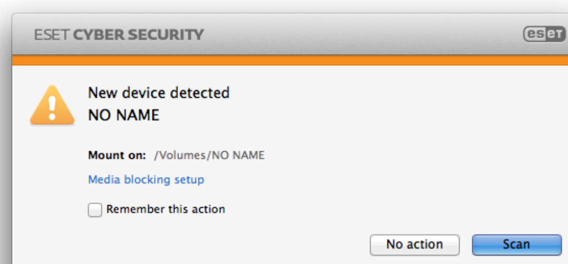
Limpeza e exclusão - Aplique a limpeza se um arquivo tiver sido atacado por um vírus que anexou a esse arquivo um código malicioso. Se esse for o caso, tente primeiro limpar o arquivo infectado a fim de restaurá-lo ao seu estado original. Se o arquivo for constituído exclusivamente por código malicioso, ele será excluído.



Exclusão de arquivos em arquivos compactados - No modo de limpeza padrão, os arquivos compactados serão excluídos somente se contiverem arquivos infectados e nenhum arquivo limpo. Em outras palavras, os arquivos compactados não serão excluídos se eles contiverem também arquivos limpos inofensivos. Entretanto, tome cuidado ao realizar um rastreamento de **Limpeza rígida**. Com esse tipo de limpeza, o arquivo será excluído se contiver pelo menos um arquivo infectado, independentemente do status dos demais arquivos contidos no arquivo compactado.

6.2 Bloqueio e rastreamento de mídia removível

O ESET Cyber Security oferece um rastreamento sob demanda do dispositivo de mídia removível inserido (CD, DVD, USB, dispositivo iOS, etc.).



A mídia removível pode conter código malicioso e colocar o computador em risco. Para bloquear mídia removível, clique no botão **Configuração de bloqueio de mídia** (veja a imagem acima) ou em **Configurar** > **Entrar nas preferências do aplicativo...** > **Mídia** na janela do programa principal e marque a opção **Ativar bloqueio de mídia removível**. Para permitir o acesso a determinados tipos de mídia, desmarque os volumes de mídia desejados.

OBSERVAÇÃO: Se você quiser permitir o acesso à unidade externa de CD-ROM conectada ao seu computador via cabo USB, desmarque a opção **CD-ROM**.

7. Proteção à web e de emails

A configuração da proteção à web e de emails pode ser encontrada em **Configurar** > **Web e email**. Você também pode acessar mais configurações detalhadas de cada módulo a partir daqui.

Proteção do acesso à web e contra phishing - se ativada (recomendado), a proteção em tempo real do sistema de arquivos monitora constantemente todos os eventos relacionados a antivírus.

Proteção de cliente de email - fornece controle da comunicação por email recebida via protocolos POP3 e IMAP.

7.1 Proteção web

A proteção de acesso à Web monitora a comunicação entre os navegadores da Internet e servidores remotos e cumpre as regras do protocolo HTTP (Hypertext Transfer Protocol).

7.1.1 Portas

Na guia **Portas**, você pode definir os números das portas utilizadas para a comunicação HTTP. Por padrão, os números de portas 80, 8080 e 3128 estão predefinidos.

7.1.2 Modo ativo

O ESET Cyber Security também contém o submenu **Modo Ativo**, que define o modo de verificação para os navegadores da web. O modo ativo examina os dados transferidos de aplicativos acessando a Internet como um todo, independentemente de eles serem marcados como navegadores da web ou não. Se não estiver ativado, a comunicação dos aplicativos é monitorada gradualmente em lotes. Isso diminui a eficiência do processo de verificação dos dados, mas também fornece maior compatibilidade para os aplicativos listados. Se nenhum problema ocorrer durante ao usá-lo, recomendamos que você ative o modo de verificação ativo marcando a caixa de seleção ao lado do aplicativo desejado.

Quando um aplicativo com acesso à rede fizer download de dados, ele será primeiro salvo em um arquivo temporário criado pelo ESET Cyber Security. Nesse momento, os dados não estão disponíveis para o aplicativo determinado. Assim que o download for concluído, ele será rastreado contra códigos maliciosos. Se não for encontrada infiltração, os dados serão enviados para o aplicativo original. Esse processo fornece controle completo das comunicações feitas por um aplicativo controlado. Se o modo passivo estiver ativado, os dados serão destinados ao aplicativo original para evitar atingir o tempo limite.

7.1.3 Listas de URL

A seção **Listas de URL** permite especificar endereços HTTP a serem bloqueados, permitidos ou excluídos da verificação. Os sites na lista de endereços bloqueados não serão acessíveis. Os sites na lista de endereços excluídos são acessados sem serem rastreados quanto a código malicioso.

Se você quiser permitir acesso somente aos endereços URL relacionados na lista **URL permitido**, selecione a opção **Restringir endereços URL**.

Para ativar uma lista, selecione a opção **Ativado**. Se você desejar ser notificado ao inserir um endereço da lista atual, selecione a opção **Notificado**.

Em todas as listas, os símbolos especiais *(asterisco) e *?* (ponto de interrogação) podem ser usados. O asterisco substitui qualquer cadeia de caracteres e o ponto de interrogação substitui qualquer símbolo. Tenha atenção especial ao especificar os endereços excluídos, uma vez que a lista deve conter os endereços seguros e confiáveis. De modo similar, é necessário assegurar que os símbolos * e ? sejam usados corretamente na lista.

7.2 Proteção de email

A proteção de email fornece controle da comunicação por email recebida via protocolos POP3 e IMAP. Ao verificar as mensagens de entrada, o programa usa todos os métodos de rastreamento avançado oferecidos pelo mecanismo de rastreamento ThreatSense. Isto significa que a detecção de programas maliciosos é realizada até mesmo antes dos mesmos serem comparados com a base de dados de assinaturas de vírus. O rastreamento de comunicações dos protocolos POP3 e IMAP é independente do cliente de email usado.

Mecanismo ThreatSense - a configuração avançada do scanner de vírus permite configurar alvos de rastreamento, métodos de detecção, etc. Clique em **Configurar...** para exibir a janela de configuração do scanner de vírus detalhada.

Depois que um email tiver sido verificado, uma notificação com o resultado da verificação pode ser anexada à mensagem. Você poderá selecionar **Anexar mensagens de marca ao assunto do email**. Não se deve confiar nas mensagens de marca sem questioná-las, pois elas podem ser omitidas em mensagens HTML problemáticas ou podem ser forjadas por alguns vírus. As opções disponíveis são:

Nunca - nenhuma mensagem de marca será adicionada,
Somente para email infectado - somente mensagens contendo software malicioso serão marcadas como rastreadas,
Para todos os emails rastreados - o programa anexará mensagens a todos os emails rastreados.

Modelo adicionado ao assunto de email infectado - edite esse modelo se desejar modificar o formato de prefixo do assunto de um email infectado.

Anexar mensagens de marca ao rodapé do email - marque

essa caixa de seleção se você quiser que a proteção de email inclua um alerta de vírus no assunto de um email infectado. Esse recurso permite a filtragem simples de emails infectados. Esse recurso aumenta o nível de credibilidade para os destinatários e, se nenhuma infiltração for detectada, ele fornece informações valiosas sobre o nível de ameaça do email ou do remetente.

7.2.1 Verificação de protocolo POP3

O protocolo POP3 é o protocolo mais amplamente utilizado para receber comunicação em um aplicativo cliente de email. O ESET Cyber Security fornece proteção a esse protocolo, independentemente do cliente de email usado.

O módulo de proteção que permite esse controle é automaticamente ativado na inicialização do sistema e fica ativo na memória. Para que o módulo funcione corretamente, verifique se ele está ativado; a verificação do protocolo POP3 é feita automaticamente, sem necessidade de reconfiguração do cliente de email. Por padrão, todas as comunicações através da porta 110 são rastreadas, mas podem ser adicionadas outras portas de comunicação, se necessário. Os números das portas devem ser delimitados por vírgula.

Se a opção **Ativar verificação de email** estiver ativada, todo o tráfego por meio do POP3 será monitorado quanto a software malicioso.

7.2.2 Verificação de protocolo IMAP

O IMAP (Internet Message Access Protocol) é outro protocolo de Internet para recuperação de emails. O IMAP tem algumas vantagens sobre o POP3, por exemplo, vários clientes podem se conectar simultaneamente à mesma caixa de correio e gerenciar informações de estado das mensagens, tais como se a mensagem foi ou não lida, respondida ou excluída. O ESET Cyber Security fornece proteção para este protocolo, independentemente do cliente de email usado.

O módulo de proteção que permite esse controle é automaticamente ativado na inicialização do sistema e fica ativo na memória. Para que o módulo funcione corretamente, verifique se ele está ativado; o controle do protocolo IMAP é feito automaticamente, sem necessidade de reconfiguração do cliente de email. Por padrão, todas as comunicações através da porta 143 são rastreadas, mas podem ser adicionadas outras portas de comunicação, se necessário. Os números das portas devem ser delimitados por vírgula.

Se a opção **Ativar verificação de protocolo IMAP** estiver ativada, todo o tráfego por meio do IMAP será monitorado quanto a software malicioso.

8. Atualizar

Atualizar o ESET Cyber Security com regularidade é necessário para manter o nível máximo de segurança. O módulo de atualização garante que o programa esteja sempre atualizado por meio de download do banco de dados de assinatura de vírus mais recente.

No menu principal, ao clicar em **Atualizar**, você poderá localizar o status da atualização atual, incluindo o dia e a hora da última atualização bem-sucedida, e se uma atualização será necessária. Para iniciar o processo de atualização manualmente, clique em **Atualizar banco de dados de assinatura de vírus**.

Em circunstâncias normais, quando o download das atualizações é feito adequadamente, a mensagem **O banco de dados de assinatura de vírus está atualizado** aparecerá na janela Atualizar. Se o banco de dados de assinatura de vírus não puder ser atualizado, recomendamos que você verifique as configurações de atualização 14. O motivo mais comum para esse erro são dados de autenticação digitados incorretamente (Usuário e Senha), ou configurações de conexão 20 incorretas.

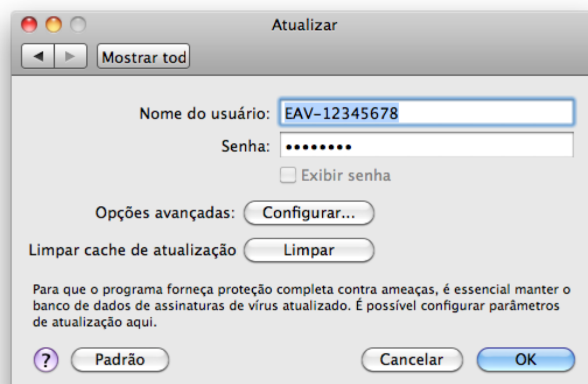
A janela Atualizar também contém informações sobre a versão o banco de dados de assinatura de vírus. Esse indicador numérico é um link ativo para o site da ESET que lista todas as assinaturas adicionadas durante determinada atualização.

OBSERVAÇÃO: O nome de usuário e a senha são fornecidos pela ESET após a compra do ESET Cyber Security.

8.1 Configuração da atualização

A autenticação dos servidores de atualização é baseada no Usuário e na Senha gerados e enviados a você após a compra.

Para ativar a utilização do modo de teste (modo de teste de downloads), clique no botão **Configurar** > **Entrar nas preferências do aplicativo...** (ou pressione *cmd-,*) > **Atualizar**, clique no botão **Configurar...** ao lado de **Opções avançadas** e marque a caixa de seleção **Ativar modo de teste**.



Para desativar as notificações da bandeja do sistema que são exibidas após cada atualização bem-sucedida, marque a caixa de seleção **Não exibir notificação sobre atualização bem-sucedida**.

Para excluir todos os dados de atualização armazenados temporariamente, clique no botão **Limpar** ao lado de **Limpar cache de atualização**. Utilize essa opção se estiver com dificuldades durante a atualização.

8.2 Como criar tarefas de atualização

As atualizações podem ser disparadas manualmente clicando em **Atualizar banco de dados de assinatura de vírus** na janela primária, exibida depois de clicar em **Atualizar** no menu principal.

As atualizações também podem ser executadas como tarefas agendadas. Para configurar uma tarefa agendada, clique em **Ferramentas** > **Agenda**. Por padrão, as seguintes tarefas estão ativadas no ESET Cyber Security:

- **Atualização automática de rotina**
- **Atualização automática após logon do usuário**

Cada uma das tarefas de atualização pode ser modificada para atender às suas necessidades. Além das tarefas de atualização padrão, você pode criar novas tarefas de atualização com uma configuração definida pelo usuário. Para obter mais detalhes sobre a criação e a configuração de tarefas de atualização, consulte a seção Agenda 16.

8.3 Atualização do ESET Cyber Security para uma nova versão

Para obter a máxima proteção, é importante usar a compilação mais recente do ESET Cyber Security. Para verificar se há uma nova versão, clique em **Início** no menu principal à esquerda. Se uma nova compilação estiver disponível, uma mensagem será exibida. Clique em **Saber mais...** para exibir uma nova janela que contenha o número da versão da nova compilação e o log de alterações.

Clique em **Sim** para fazer download da compilação mais recente ou em **Agora não** para fechar a janela e fazer download da atualização mais tarde.

Se você clicou em **Sim**, o arquivo será obtido por download para a sua pasta de downloads (ou para a pasta padrão definida pelo navegador). Quando o download do arquivo estiver concluído, inicie o arquivo e siga as instruções de instalação. O seu nome de usuário e a sua senha serão automaticamente transferidos para a nova instalação. É recomendável verificar se há atualizações regularmente, especialmente quando instalar o ESET Cyber Security usando CD ou DVD.

9. Ferramentas

O menu **Ferramentas** inclui módulos que ajudam a simplificar a administração do programa e oferecem opções adicionais para usuários avançados.

9.1 Arquivos de log

Os arquivos de log contêm informações sobre todos os eventos importantes do programa que ocorreram e fornecem uma visão geral das ameaças detectadas. O registro em log atua como uma ferramenta essencial na análise do sistema, na detecção de ameaças e na solução de problemas. O registro em log realiza-se ativamente em segundo plano, sem interação do usuário. As informações são registradas com base nas configurações atuais do detalhamento do log. É possível visualizar mensagens de texto e logs diretamente do ambiente do ESET Cyber Security, bem como arquivar logs.

Os arquivos de log podem ser acessados no menu principal do ESET Cyber Security, clicando em **Ferramentas** > **Relatórios**. Selecione o tipo de log desejado, utilizando o menu suspenso **Log** na parte superior da janela. Os seguintes relatórios estão disponíveis:

1. **Ameaças detectadas** – use essa opção para exibir todas as informações sobre eventos relacionados à detecção de infiltrações.
2. **Eventos** - essa opção foi desenvolvida para a solução de problemas de administradores do sistema e usuários. Todas as ações importantes executadas pelo ESET Cyber Security são registradas nos logs de eventos.
3. **Rastrear o computador** - os resultados de todos os rastreamentos concluídos são exibidos nessa janela. Clique duas vezes em qualquer entrada para exibir os detalhes do respectivo Rastreamento sob demanda do computador.

Em cada seção, as informações exibidas podem ser copiadas diretamente para a área de transferência, selecionando a entrada e clicando no botão **Copiar**.

9.1.1 Manutenção de logs

A configuração de logs do ESET Cyber Security pode ser acessada na janela principal do programa. Clique em **Configuração** > **Entrar nas preferências do aplicativo ...** (ou pressione *cmd-,*) > **Arquivos de log**. Você pode especificar as seguintes opções para logs:

- **Excluir logs antigos automaticamente** - as entradas de logs anteriores ao número de dias especificado são automaticamente excluídas.
- **Otimizar automaticamente logs** - ativa a desfragmentação automática de logs se a porcentagem especificada de logs não utilizados foi excedida.

Para configurar o **Filtro padrão dos logs**, clique no botão **Editar...** e marque/desmarque os tipos de logs, conforme a necessidade.

9.1.2 Filtragem de logs

Registra em logs as informações de armazenamento sobre eventos importantes do sistema. O recurso de filtragem de logs permite exibir registros sobre um tipo específico de evento.

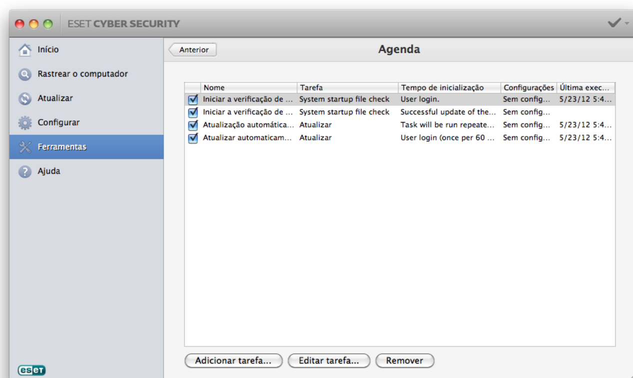
Os tipos de logs utilizados com mais frequência são listados a seguir:

- **Avisos críticos** - erros críticos do sistema (por exemplo, falha em iniciar a proteção antivírus)
- **Erros** - mensagens de erro, como "*Erro ao fazer download de arquivo*" e erros críticos
- **Avisos** - mensagens de avisos

- **Registros informativos** - mensagens informativas, incluindo atualizações bem sucedidas, alertas, etc.
- **Registros de diagnóstico** - informações necessárias para ajustar o programa e também todos os registros descritos acima.

9.2 Agenda

A **Agenda** pode ser encontrada no menu principal do ESET Cyber Security em **Ferramentas**. A **Agenda** contém uma lista de todas as tarefas agendadas e suas propriedades de configuração, como a data e a hora predefinidas e o perfil de rastreamento utilizado.



A Agenda gerencia e inicia tarefas agendadas com as configurações e propriedades predefinidas. A configuração e as propriedades contêm informações, como a data e o horário, bem como os perfis especificados para serem utilizados durante a execução da tarefa.

Por padrão, as seguintes tarefas agendadas são exibidas na Agenda:

- Manutenção de relatórios (após a ativação da opção **Mostras as tarefas do sistema** na configuração da agenda)
- Rastreamento de arquivos durante inicialização do sistema após logon do usuário
- Rastreamento de arquivos durante inicialização do sistema após atualização bem sucedida do banco de dados de assinatura de vírus
- Atualização automática de rotina
- Atualização automática após logon do usuário

Para editar a configuração de uma tarefa agendada existente (tanto padrão quanto definida pelo usuário), pressione ctrl, clique na tarefa que você deseja modificar e selecione **Editar...** ou selecione a tarefa e clique no botão **Editar tarefa...**.

9.2.1 Criação de novas tarefas

Para criar uma nova tarefa na Agenda, clique no botão **Adicionar tarefa...** ou pressione ctrl, clique no campo em branco e selecione **Adicionar...** no menu de contexto. Cinco tipos de tarefas agendadas estão disponíveis:

- **Executar aplicativo**
- **Atualizar**
- **Manutenção de logs**
- **Rastreamento sob demanda do computador**
- **Rastrear arquivos na inicialização do sistema**

Como Atualizar é uma das tarefas agendadas usadas com mais frequência, nós explicaremos como adicionar uma nova tarefa de atualização.

No menu suspenso **Tarefa agendada**, selecione **Atualizar**. Digite o nome da tarefa no campo **Nome da tarefa**. Selecione a frequência da tarefa no menu suspenso **Executar tarefa**. Com base na frequência selecionada, diferentes parâmetros de atualização serão exibidos para você.

Se selecionar **Definida pelo usuário**, você será solicitado a especificar uma data/hora no formato cron (consulte a seção Criar regra definida pelo usuário 16 para obter mais detalhes).

Na próxima etapa, defina a ação a ser tomada se a tarefa não puder ser executada ou concluída na hora agendada. As três opções a seguir estão disponíveis:

- **Aguardar até a próxima hora agendada**
- **Executar a tarefa tão logo quanto possível**
- **Executar a tarefa imediatamente se a hora desde a última execução exceder o intervalo especificado** (o intervalo pode ser definido utilizando a opção **Intervalo mínimo da tarefa**)

Na próxima etapa, uma janela de resumo com as informações sobre a tarefa agendada atual será exibida. Clique no botão **Concluir**.

A nova tarefa agendada será adicionada à lista de tarefas agendadas no momento.

O sistema, por padrão, contém as tarefas agendadas necessárias para garantir a funcionalidade correta do produto. Elas não devem ser alteradas e ficam ocultas, por padrão. Para alterar essa opção e tornar essas tarefas visíveis, entre em **Configurar** > **Entrar nas preferências do aplicativo ...** (ou pressione *cmd-,*) > **Agenda** e selecione a opção **Mostrar tarefas do sistema**.

9.2.2 Criação de regra definida pelo usuário

A data e hora da tarefa **Definida pelo usuário** precisam ser inseridas em um formato cron de ano estendido (uma cadeia de caracteres incluindo 6 campos separados por um espaço em branco):

```
minuto(0-59) hora(0-23) dia do mês(1-31) mês(1-12)
ano(1970-2099) dia da semana(0-7)(Domingo = 0 ou 7)
```

Exemplo:

```
30 6 22 3 2012 4
```

Caracteres especiais suportados em expressões cron:

- asterisco (`*`) - a expressão irá corresponder para todos os valores no campo; por exemplo, um asterisco no terceiro campo (dia do mês) significa todo dia
- hífen (`-`) - define intervalos; por exemplo, `3-9`
- vírgula (`,`) - separa os itens de uma lista; por exemplo, `1,3,7,8`
- barra (`/`) - define incrementos de intervalos; por exemplo, `3-28/5` no terceiro campo (dia do mês) significa o 3.º dia do mês e a cada 5 dias.

Os nomes dos dias (Monday-Sunday) e dos meses (January-December) não são suportados.

OBSERVAÇÃO: Se você definir o dia do mês e o dia da semana, o comando será executado somente quando ambos os campos corresponderem.

9.3 Quarentena

A principal tarefa da quarentena é armazenar os arquivos infectados de maneira segura. Os arquivos devem ser colocados em quarentena se não puderem ser limpos, se não for seguro nem aconselhável excluí-los ou se eles estiverem sendo falsamente detectados pelo ESET Cyber Security.

Você pode optar por colocar qualquer arquivo em quarentena. É aconselhável colocar um arquivo em quarentena se ele se comportar de modo suspeito, mas não for detectado pelo verificador antivírus. Os arquivos colocados em quarentena podem ser enviados ao Laboratório de ameaças da ESET para análise.

Os arquivos armazenados na pasta de quarentena podem ser visualizados em uma tabela que exibe a data e o horário da quarentena, o caminho para o local original do arquivo infectado, o tamanho do arquivo em bytes, a razão (por exemplo, adicionado pelo usuário...) e o número de ameaças (por exemplo, se for um arquivo compactado que contém diversas ameaças). A pasta de quarentena com os arquivos colocados em quarentena (*/Library/Application Support/Eset/esets/cache/quarantine*) permanece no sistema mesmo depois da desinstalação do ESET Cyber Security. Os arquivos em quarentena são armazenados em um formato criptografado e seguro e podem ser restaurados novamente após a instalação do ESET Cyber Security.

9.3.1 Colocação de arquivos em quarentena

O ESET Cyber Security coloca automaticamente os arquivos excluídos em quarentena (se você não cancelou essa opção na janela de alertas). Se desejar, é possível colocar manualmente em quarentena qualquer arquivo suspeito clicando no botão **Quarentena...**. O menu de contexto pode ser utilizado também para essa finalidade - pressione ctrl, clique no campo em branco, selecione **Quarentena...**, escolha o arquivo que deseja colocar em quarentena e clique no botão **Abrir**.

9.3.2 Restauração da Quarentena

Os arquivos colocados em quarentena podem também ser restaurados para o local original. Use o botão **Restaurar** para essa finalidade; Restaurar também está disponível no menu de contexto pressionando ctrl, clicando no arquivo determinado na janela Quarentena, e então, clicando em **Restaurar**. O menu de contexto oferece também a opção **Restaurar para...**, que permite restaurar um arquivo para um local diferente do local original do qual ele foi excluído.

9.3.3 Envio de arquivo da Quarentena

Se você colocou em quarentena um arquivo suspeito não detectado pelo programa, ou se um arquivo foi avaliado incorretamente como infectado (por exemplo, pela análise heurística do código) e colocado em quarentena, envie o arquivo ao Laboratório de ameaças da ESET. Para enviar um arquivo diretamente da quarentena, pressione ctrl, clique no arquivo e selecione **Enviar arquivo para análise** do menu de contexto.

9.4 Processos em execução

A lista de **Processos em execução** exibe os processos em execução em seu computador. O ESET Cyber Security fornece informações detalhadas sobre processos em execução para proteger usuários com a tecnologia ESET Live Grid.

- **Processo** - nome do processo que está atualmente em execução em seu computador. Para ver todos os processos em execução, você também pode usar o Monitor de atividade (encontrado em */Aplicativos/Utilitários*).
- **Nível de risco** - na maioria dos casos, o ESET Cyber Security e a tecnologia ESET Live Grid atribuem níveis de risco a objetos (arquivos, processos, etc.) usando uma série de regras heurísticas que examinam as características de cada objeto e então avaliam o potencial de atividade mal-intencionada. Com base nessa heurística, os objetos recebem um nível de risco. Os aplicativos conhecidos marcados em verde estão definitivamente limpos (na lista de permissões) e serão excluídos do rastreamento. Isso aprimorará a velocidade de rastreamento sob demanda e em tempo real. Quando um aplicativo é marcado como desconhecido (em amarelo), ele não é necessariamente software mal-intencionado. Geralmente, é apenas um aplicativo mais recente. Se você não estiver certo em relação ao arquivo, poderá enviá-lo para análise ao Laboratório de ameaças da ESET. Se for descoberto que o arquivo é um aplicativo mal-intencionado, sua detecção será adicionada em uma das próximas atualizações.
- **Número de usuários** - o número de usuários que usam determinado aplicativo. Essas informações são coletadas pela tecnologia ESET Live Grid.
- **Hora da descoberta** - período de tempo desde que o aplicativo foi descoberto pela tecnologia ESET Live Grid.
- **ID do pacote do aplicativo** - nome do fornecedor ou processo de aplicativo.

Ao clicar em determinado processo, as seguintes informações serão exibidas na parte inferior da janela:

- **Arquivo** - local de um aplicativo em seu computador,
- **Tamanho do arquivo** - tamanho físico do arquivo no disco,
- **Descrição do arquivo** - características do arquivo com base na descrição do sistema operacional,
- **ID do pacote do aplicativo** - nome do fornecedor ou processo de aplicativo,
- **Versão do arquivo** - informações do editor do aplicativo,
- **Nome do produto** - nome do aplicativo e/ou nome comercial.

9.5 Live Grid

O Live Grid Early Warning System mantém a ESET, imediatamente e continuamente, informada sobre novas infiltrações. O sistema de alerta bidirecional do Live Grid Early Warning System tem uma única finalidade: melhorar a proteção que podemos proporcionar-lhe. A melhor maneira de garantir que veremos novas ameaças assim que elas aparecerem é mantermos "link" com o máximo possível de nossos clientes e usá-los como nossos Sentinelas de ameaças. Há duas opções:

1. Você pode decidir não ativar o Live Grid Early Warning System. Você não perderá nenhuma funcionalidade do software e ainda receberá a melhor proteção que oferecemos.
2. É possível configurar o Live Grid Early Warning System para enviar informações anônimas sobre as novas ameaças e onde o novo código de ameaça está contido. Esse arquivo pode ser enviado para a ESET para análise detalhada. O estudo dessas ameaças ajudará a ESET a atualizar seu banco de dados de ameaças e melhorar a capacidade de detecção do programa.

O Live Grid Early Warning System coletará informações sobre o seu computador relacionadas a ameaças recém-detectadas. Essas informações podem incluir uma amostra ou cópia do arquivo no qual a ameaça apareceu, o caminho para o arquivo, o nome do arquivo, a data e a hora, o processo pelo qual a ameaça apareceu no computador e as informações sobre o sistema operacional do seu computador.

Enquanto há uma possibilidade de que isso possa ocasionalmente revelar algumas informações sobre você ou seu computador (usuários em um caminho de diretório, etc.) para o Laboratório de ameaças da ESET, essas informações não serão utilizadas para QUALQUER outra finalidade que não seja nos ajudar a reagir imediatamente contra novas ameaças.

A configuração do Live Grid está acessível em **Configurar** > **Entrar nas preferências do aplicativo...** (ou pressione *cmd-,*) > **Live Grid**. Selecione a opção **Ativar Live Grid Early Warning System** para ativar e então clique no botão **Configurar...**, ao lado do cabeçalho **Opções avançadas**.

9.5.1 Configuração do Live Grid

Por padrão, o ESET Cyber Security é configurado para enviar arquivos suspeitos ao Laboratório de ameaças da ESET para análise detalhada. Se você não quiser enviar esses arquivos automaticamente, desmarque a opção **Envio de arquivos suspeitos**.

Se encontrar um arquivo suspeito, você poderá enviá-lo ao nosso Laboratório de ameaças para análise. Para fazer isso, clique em **Ferramentas** > **Enviar arquivo para análise** na janela principal do programa. Se for um aplicativo malicioso, sua detecção será adicionada à próxima atualização de assinaturas de vírus.

Envio de informações estatísticas anônimas - o ESET Live Grid Early Warning System coleta informações anônimas sobre seu computador relacionadas a ameaças detectadas recentemente. Essas informações incluem o nome da ameaça, a data e o horário em que ela foi detectada, a versão do produto de segurança da ESET, a versão do seu sistema operacional e a configuração de local. As estatísticas são normalmente enviadas aos servidores da ESET, uma ou duas vezes por dia.

A seguir há um exemplo de um pacote estatístico enviado:

```
# utc_time=2005-04-14 07:21:28
# country="Slovakia"
# language="ENGLISH"
# osver=9.5.0
# engine=5417
# components=2.50.2
# moduleid=0x4e4f4d41
# filesize=28368
# filename=Users/UserOne/Documents/Incoming/rdgFR1463
[1].zip
```

Filtro de exclusões - Essa opção permite excluir determinados arquivos do envio. Por exemplo, pode ser útil excluir arquivos que podem conter informações sigilosas, como documentos ou planilhas. Os tipos de arquivos mais comuns são excluídos por padrão (.doc, .rtf, etc.). Você pode adicionar os tipos de arquivos à lista de arquivos excluídos.

Email de contato (opcional) - seu endereço de email será utilizado se precisarmos de mais informações para análise. Observe que você não receberá uma resposta da ESET, a menos que mais informações sejam necessárias.

10. Interface do usuário

As opções de configuração da interface do usuário permitem que você ajuste o ambiente de trabalho para que ele atenda às suas necessidades. Essas opções podem ser acessadas em **Configurar** > **Entrar nas preferências do aplicativo...** (ou pressione *cmd-,*) > **Interface**.

Para exibir a tela inicial do ESET Cyber Security na inicialização do sistema, selecione a opção **Mostrar tela inicial na inicialização**.

A opção **Aplicativo presente no Dock** permite que você exiba o ícone ESET Cyber Security no Mac OS Dock e alterne entre o ESET Cyber Security e outros aplicativos em execução pressionando *cmd-tab*. As alterações serão implementadas

depois que você reiniciar o ESET Cyber Security (geralmente acionado pela reinicialização do computador).

A opção **Usar menu padrão** permite que você use determinadas teclas de atalho do teclado (consulte Teclas de atalho do teclado 6) e veja itens de menu padrão (Interface do usuário, Configuração e Ferramentas) na barra de menu do Mac OS (início da tela).

Para ativar dicas de ferramentas para determinar opções do ESET Cyber Security, selecione a opção **Mostrar dicas de ferramentas**.

A opção **Mostrar arquivos ocultos** permite que você veja e selecione arquivos ocultos na configuração **Alvos de rastreamento** de um **Rastrear o computador**.

10.1 Alertas e notificações

A seção **Alertas e notificações** permite que você configure a maneira como os alertas de ameaças e as notificações do sistema são tratados no ESET Cyber Security.

A desativação da opção **Exibir alertas** cancelará todas as janelas de alertas e será adequada somente para situações específicas. Para a maioria dos usuários, recomendamos que essa opção seja mantida como a configuração padrão (ativada).

A seleção da opção **Exibir notificações na área de trabalho** ativará as janelas de alertas que não exigem a interação do usuário para serem exibidas na área de trabalho (por padrão, no canto superior direito da sua tela). Você pode definir o período no qual a notificação será exibida, ajustando o valor de **Fechar notificações automaticamente depois de** X **segundos**.

Se você quiser exibir somente notificações que requerem interação do usuário ao executar aplicativos em modo de tela inteira, marque a opção **Ativar o modo de tela cheia**. Isso é útil durante apresentações, jogos ou outras atividades que exijam o modo de tela cheia.

10.1.1 Configuração avançada de alertas e notificações

O ESET Cyber Security exibe janelas da caixa de diálogo de alerta, informando você sobre a nova versão do programa, nova atualização de SO, desativando determinados componentes do programa, excluindo relatórios, etc. Você pode suprimir cada notificação selecionando a opção **Não exibir essa janela de diálogo novamente** em cada janela da caixa de diálogo.

Lista de caixas de diálogos (**Configurar** > **Entrar nas preferências do aplicativo...** > **Alertas e notificações** > **Configurar...**) mostra a lista de todas as caixas de diálogo de alerta acionadas pelo ESET Cyber Security. Para ativar ou suprimir cada notificação, use a caixa de seleção à esquerda de **Nome da notificação**. Além disso, você pode definir **Condições de exibição** nas quais as notificações sobre nova versão de programa e atualização de SO serão exibidas.

10.2 Privilégios

As configurações do ESET Cyber Security podem ser muito importantes para a política de segurança da organização. Modificações não autorizadas podem pôr em risco a estabilidade e a proteção do seu sistema. Consequentemente, você pode escolher quais usuários terão permissão para editar a configuração do programa.

Para especificar os usuários privilegiados, clique em **Configurar** > **Entrar nas preferências do aplicativo...** (ou pressione *cmd-,*) > **Privilégios**.

Para fornecer segurança máxima ao seu sistema, é fundamental que o programa seja configurado corretamente. Modificações não autorizadas podem resultar na perda de dados importantes. Para definir uma lista de usuários privilegiados, basta selecioná-los na lista **Usuários** do lado esquerdo e clicar no botão **Adicionar**. Para exibir todos os usuários do sistema, selecione a opção **Mostrar todos os usuários**. Para remover um usuário, basta selecionar o seu nome na lista **Usuários privilegiados** do lado direito e clicar em **Remover**.

OBSERVAÇÃO: Se a lista de usuários privilegiados estiver vazia, todos os usuários do sistema terão permissão para editar as configurações do programa.

10.3 Menu de contexto

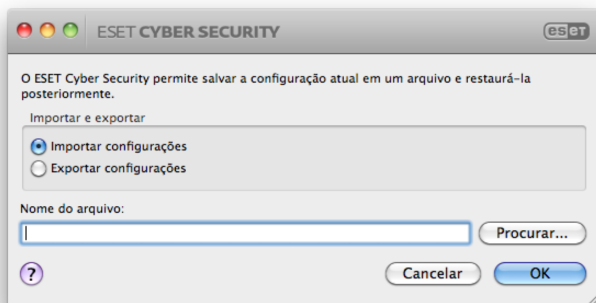
A integração do menu de contexto pode ser ativada na seção **Configurar** > **Entrar nas preferências do aplicativo...** (ou pressione *cmd-,* > **Menu de contexto**, selecionando-se a opção **Integrar ao menu de contexto**. O logout ou reinicialização do computador é necessário para que as alterações sejam implementadas. As opções do menu de contexto estarão disponíveis na janela **Finder** quando você pressionar o botão ctrl e clicar em qualquer arquivo.

11. Diversos

11.1 Importar e exportar configurações

A importação e a exportação das configurações do ESET Cyber Security estão disponíveis no painel **Configurar**.

A Importação e a Exportação utilizam arquivos compactados para armazenar a configuração. A importação e a exportação serão úteis caso precise fazer backup da configuração atual do ESET Cyber Security para que ela possa ser utilizada posteriormente. A opção de exportação de configurações também é conveniente para os usuários que desejam utilizar as suas configurações preferenciais do ESET Cyber Security em diversos sistemas. Os usuários também podem importar o arquivo de configuração para transferir as configurações desejadas.



11.1.1 Importar configurações

Para importar uma configuração, clique em **Configuração** > **Importar e exportar configurações...** no menu principal e selecione a opção **Importar configurações**. Digite o nome do arquivo de configuração ou clique no botão **Procurar...** para procurar o arquivo de configuração que deseja importar.

11.1.2 Exportar configurações

Para exportar uma configuração, clique em **Configuração** > **Importar e exportar configurações...** no menu principal. Selecione a opção **Exportar configurações** e digite o nome do arquivo de configuração. Utilize o navegador para selecionar um local no computador no qual deseja salvar o arquivo de configuração.

11.2 Configuração do servidor proxy

As configurações do servidor proxy podem ser definidas em **Configurar** > **Entrar nas preferências do aplicativo...** (ou pressione *cmd-,*) > **Servidor proxy**. A especificação do servidor proxy neste nível define as configurações globais do servidor proxy para todas as funções do ESET Cyber Security. Aqui os parâmetros serão utilizados por todos os módulos que exigem conexão com a Internet.

Para especificar as configurações do servidor proxy para esse nível, marque a caixa de seleção **Usar servidor proxy** e insira o endereço IP ou o URL do servidor proxy no campo **Servidor proxy**. No campo **Porta**, especifique a porta em que o servidor proxy aceita as conexões (3128 por padrão).

Se a comunicação com o servidor proxy exigir autenticação, marque a caixa de seleção **O servidor proxy requer autenticação** e digite um **Usuário** e uma **Senha** válidos nos respectivos campos.

12. Glossário

12.1 Tipos de infiltração

Uma infiltração é uma parte do software malicioso que tenta entrar e/ou danificar o computador de um usuário.

12.1.1 Vírus

Um vírus de computador é uma infiltração que corrompe os arquivos existentes em seu computador. O nome vírus vem do nome dos vírus biológicos, uma vez que eles usam técnicas semelhantes para se espalhar de um computador para outro.

Os vírus de computador atacam principalmente arquivos, scripts e documentos executáveis. Para se replicar, um vírus anexa seu "corpo" ao final de um arquivo de destino. Em resumo, é assim que um vírus de computador funciona: após a execução do arquivo infectado, o vírus ativa a si próprio (antes do aplicativo original) e realiza sua tarefa predefinida. Somente depois disso, o aplicativo original pode ser executado. Um vírus não pode infectar um computador a menos que um usuário (acidental ou deliberadamente) execute ou abra o programa malicioso.

Os vírus de computador podem se ampliar em finalidade e gravidade. Alguns deles são extremamente perigosos devido à sua capacidade de propositalmente excluir arquivos do disco rígido. Por outro lado, alguns vírus não causam danos reais; eles servem somente para perturbar o usuário e demonstrar as habilidades técnicas dos seus autores.

É importante observar que os vírus (quando comparados a cavalos de troia ou spyware) estão se tornando cada vez mais raros, uma vez que eles não são comercialmente atrativos para os autores de softwares maliciosos. Além disso, o termo "vírus" é frequentemente usado de maneira incorreta para cobrir todos os tipos de infiltrações. Essa utilização está gradualmente sendo superada e substituída pelo novo e mais preciso termo "malware" (software malicioso).

Se o seu computador estiver infectado por um vírus, será necessário restaurar os arquivos infectados para o seu estado original, ou seja, limpá-los usando um programa antivírus.

12.1.2 Worms

Um worm de computador é um programa contendo código malicioso que ataca os computadores host e se espalha pela rede. A diferença básica entre um vírus e um worm é que os worms têm a capacidade de se replicar e viajar por conta própria; eles não dependem dos arquivos host (ou dos setores de inicialização). Os worms são propagados por meio dos endereços de email da sua lista de contatos ou aproveitam-se das vulnerabilidades da segurança dos aplicativos de rede.

Os worms são, portanto, muito mais férteis do que os vírus de computador. Devido à ampla disponibilidade da Internet, eles podem se espalhar por todo o globo dentro de horas após sua liberação – em alguns casos, até em minutos. Essa capacidade de se replicar independentemente e de modo rápido os torna mais perigosos que outros tipos de malware.

Um worm ativado em um sistema pode causar diversos transtornos: Ele pode excluir arquivos, prejudicar o desempenho do sistema ou até mesmo desativar programas. A natureza de um worm de computador o qualifica como um "meio de transporte" para outros tipos de infiltrações.

Se o seu computador foi infectado por um worm, recomendamos que exclua os arquivos infectados porque eles provavelmente conterão códigos maliciosos.

12.1.3 Cavalos de troia (Trojans)

Historicamente, os cavalos de troia dos computadores foram definidos como uma classe de infiltrações que tenta se apresentar como programas úteis, enganando assim os usuários que os deixam ser executados. Hoje não há mais a necessidade de cavalos de troia para que eles se disfarcem. O seu único propósito é se infiltrar o mais facilmente possível e cumprir com seus objetivos maliciosos. O "cavalo de troia" tornou-se um termo muito genérico para descrever qualquer infiltração que não se encaixe em uma classe específica de infiltração.

Uma vez que essa é uma categoria muito ampla, ela é frequentemente dividida em muitas subcategorias:

- Downloader – Um programa malicioso com a capacidade de fazer o download de outras infiltrações da Internet.
- Dropper – Um tipo de cavalo de troia projetado para instalar outros tipos de malware em computadores comprometidos.
- Backdoor – Um aplicativo que se comunica com agressores remotos, permitindo que eles obtenham acesso a um sistema e assumam o controle dele.
- Keylogger – (keystroke logger) – Um programa que registra cada toque na tecla que o usuário digita e envia as informações para os agressores remotos.
- Dialer – Dialers são programas projetados para se conectar aos números premium-rate. É quase impossível para um usuário notar que uma nova conexão foi criada. Os dialers somente podem causar danos aos usuários com modens discados que não são mais usados regularmente.
- Os cavalos de troia geralmente tomam a forma de arquivos executáveis. Se um arquivo em seu computador for detectado como um cavalo de troia, recomendamos excluí-lo, uma vez que é muito provável que ele contenha códigos maliciosos.

12.1.4 Rootkits

Os rootkits são programas maliciosos que concedem aos agressores da Internet acesso ao sistema, ao mesmo tempo que ocultam a sua presença. Os rootkits, após acessar um sistema (geralmente explorando uma vulnerabilidade do sistema) usam as funções do sistema operacional para evitar serem detectados pelo software antivírus: eles ocultam processos e arquivos. Por essa razão, é quase impossível detectá-los usando as técnicas comuns.

Há dois níveis de detecção para impedir rootkits:

1. Quando eles tentam acessar um sistema. Eles ainda não estão presentes e estão, portanto, inativos. A maioria dos sistemas antivírus são capazes de eliminar rootkits nesse nível (presumindo-se que eles realmente detectem tais arquivos como estando infectados).
2. Quando eles estão ocultos em testes comuns.

12.1.5 Adware

Adware é a abreviação de advertising-supported software (software suportado por propaganda). Os programas exibindo material de publicidade pertencem a essa categoria. Os aplicativos adware geralmente abrem automaticamente uma nova janela pop-up, contendo publicidade em um navegador da Internet, ou mudam a homepage do mesmo. O adware é frequentemente vinculado a programas freeware, permitindo que os desenvolvedores de programas freeware cubram os custos de desenvolvimento de seus aplicativos (geralmente úteis).

O adware por si só não é perigoso; os usuários somente serão incomodados pela publicidade. O perigo está no fato de que o adware também pode realizar funções de rastreamento (assim como o spyware faz).

Se você decidir usar um produto freeware, preste especial atenção ao programa de instalação. É muito provável que o instalador notifique você sobre a instalação de um programa adware extra. Normalmente você poderá cancelá-lo e instalar o programa sem o adware.

Determinados programas não serão instalados sem o adware, ou as suas funcionalidades ficarão limitadas. Isso significa que o adware acessará com frequência o sistema de modo "legal" porque os usuários concordaram com isso. Nesse caso, é melhor prevenir do que remediar. Se um arquivo for detectado como adware em seu computador, é aconselhável excluí-lo, uma vez que há uma grande probabilidade de ele conter códigos maliciosos.

12.1.6 Spyware

Essa categoria cobre todos os aplicativos que enviam informações privadas sem o consentimento/conhecimento do usuário. Os spywares usam as funções de rastreamento para enviar diversos dados estatísticos, como listas dos sites visitados, endereços de email da lista de contatos do usuário ou uma lista das teclas registradas.

Os autores de spyware alegam que essas técnicas têm por objetivo saber mais sobre as necessidades e os interesses dos usuários e permitir a publicidade mais bem direcionada. O problema é que não há uma distinção clara entre os aplicativos maliciosos e os úteis, e ninguém pode assegurar que as informações recebidas não serão usadas de modo indevido. Os dados obtidos pelos aplicativos spyware podem conter códigos de segurança, PINs, números de contas bancárias, etc. O Spyware frequentemente é vinculado a versões gratuitas de um programa pelo seu autor a fim de gerar lucro ou para oferecer um incentivo à compra do software. Geralmente, os usuários são informados sobre a presença do spyware durante a instalação do programa, a fim de fornecer a eles um incentivo para atualizar para uma versão paga sem ele.

Os exemplos de produtos freeware bem conhecidos que vêm vinculados a spyware são os aplicativos cliente das redes P2P (peer-to-peer). O Spyfalcon ou Spy Sheriff (e muitos mais) pertencem a uma subcategoria de spyware específica; eles parecem ser programas antispyware, mas são, na verdade, spyware eles mesmos.

Se um arquivo for detectado como spyware em seu computador, nós recomendamos excluí-lo, uma vez que há uma grande probabilidade de ele conter códigos maliciosos.

12.1.7 Arquivos potencialmente inseguros

Há muitos programas legítimos que têm a função de simplificar a administração dos computadores conectados em rede. Entretanto, se em mãos erradas, eles podem ser usados indevidamente para fins maliciosos. O ESET Cyber Security fornece a opção de detectar tais ameaças.

Aplicativos potencialmente inseguros é a classificação usada para software comercial legítimo. Essa classificação inclui programas como as ferramentas de acesso remoto, aplicativos para quebra de senha e keyloggers (um programa que registra cada toque na tecla que o usuário digita).

Se você achar que há um aplicativo potencialmente inseguro presente e sendo executado em seu computador (e que você não instalou), consulte o seu administrador de rede ou remova o aplicativo.

12.1.8 Aplicativos potencialmente indesejados

Aplicativos potencialmente indesejados não são necessariamente maliciosos, mas podem afetar negativamente o desempenho do computador. Tais aplicativos geralmente exigem o consentimento para a instalação. Se eles estiverem presentes em seu computador, o sistema se comportará de modo diferente (em comparação ao modo anterior à instalação desses aplicativos). As alterações mais significativas são:

- são abertas novas janelas que você não via anteriormente
- ativação e execução de processos ocultos
- uso aumentado de recursos do sistema
- alterações nos resultados de pesquisa
- o aplicativo se comunica com servidores remotos.

12.2 Tipos de ataques remotos

Há muitas técnicas especiais que permitem que os agressores comprometam os sistemas remotos. Elas são divididas em diversas categorias.

12.2.1 Ataques DoS

DoS, ou Denial of Service (negação de serviço), é a tentativa de impedir que o computador ou a rede sejam acessados por seus usuários. A comunicação entre os usuários afetados é obstruída e não pode mais continuar de modo funcional. Os computadores expostos aos ataques DoS geralmente precisam ser reinicializados para que voltem a funcionar adequadamente.

Na maioria dos casos, os alvos são servidores web e o objetivo é torná-los indisponíveis aos usuários por um determinado período de tempo.

12.2.2 Envenenamento de DNS

Através do envenenamento de DNS (Domain Name Server), os hackers podem levar o servidor DNS de qualquer computador a acreditar que os dados falsos que eles forneceram são legítimos e autênticos. As informações falsas são armazenadas em cache por um determinado período de tempo, permitindo que os agressores reescrevam as respostas do DNS dos endereços IP. Como resultado, os usuários que tentarem acessar os websites da Internet farão o download de vírus ou worms no lugar do seu conteúdo original.

12.2.3 Ataques de worm

Um worm de computador é um programa contendo código malicioso que ataca os computadores host e se espalha pela rede. Os worms de rede aproveitam-se das vulnerabilidades da segurança em vários aplicativos. Devido à disponibilidade da Internet, eles podem se espalhar por todo o globo dentro de horas após sua liberação. Em alguns casos, até mesmo em minutos.

A maioria dos ataques dos worms (Sasser, SqlSlammer) podem ser evitados usando-se as configurações de segurança padrão do firewall, ou bloqueando as portas não usadas e desprotegidas. Também é fundamental manter o sistema operacional atualizado com os patches de segurança mais

recentes.

12.2.4 Rastreamento de portas

O rastreamento de portas é usado para determinar se há portas abertas no computador em um host de rede. Um rastreador de porta é um software desenvolvido para encontrar tais portas.

Uma porta de computador é um ponto virtual que lida com os dados de entrada e saída - ação crucial do ponto de vista da segurança. Em uma rede grande, as informações reunidas pelos rastreadores de porta podem ajudar a identificar as vulnerabilidades em potencial. Esse uso é legítimo.

O rastreamento de porta é frequentemente usado pelos hackers na tentativa de comprometer a segurança. Seu primeiro passo é enviar pacotes para cada porta. Dependendo do tipo de resposta, é possível determinar quais portas estão em uso. O rastreamento por si só não causa danos, mas esteja ciente de que essa atividade pode revelar as vulnerabilidades em potencial e permitir que os agressores assumam o controle remoto dos computadores.

Os administradores de rede são aconselhados a bloquear todas as portas não usadas e proteger as que estão em uso contra o acesso não autorizado.

12.2.5 Dessincronização TCP

A dessincronização TCP é uma técnica usada nos ataques do TCP Hijacking. Ela é acionada por um processo no qual o número sequencial dos pacotes recebidos difere do número sequencial esperado. Os pacotes com um número sequencial inesperado são dispensados (ou salvos no armazenamento do buffer, se estiverem presentes na janela de comunicação atual).

Na dessincronização, os dois pontos finais da comunicação dispensam os pacotes recebidos; esse é o ponto onde os agressores remotos são capazes de se infiltrar e fornecer pacotes com um número sequencial correto. Os agressores podem até manipular ou modificar a comunicação.

Os ataques TCP Hijacking têm por objetivo interromper as comunicações servidor-cliente ou peer-to-peer. Muitos ataques podem ser evitados usando autenticação para cada segmento TCP. Também é aconselhável usar as configurações recomendadas para os seus dispositivos de rede.

12.2.6 SMB Relay

O Relé SMB e o Relé SMB 2 são programas especiais capazes de executar um ataque contra computadores remotos. Os programas se aproveitam do protocolo de compartilhamento do arquivo Server Message Block que é embutido no NetBios. Se um usuário compartilhar qualquer pasta ou diretório dentro da LAN, provavelmente ele utilizará esse protocolo de compartilhamento de arquivo.

Dentro da comunicação de rede local, as criptografias da senha são alteradas.

O Relé SMB recebe uma conexão nas portas UDP 139 e 445, detecta os pacotes trocados pelo cliente e o servidor e os modifica. Após conectar e autenticar, o cliente é desconectado. O Relé SMB cria um novo endereço IP virtual. O Relé SMB detecta a comunicação do protocolo SMB, exceto para negociação e autenticação. Os agressores remotos podem usar o endereço IP enquanto o computador cliente estiver conectado.

O Relé SMB 2 funciona com o mesmo princípio do Relé SMB, exceto que ele usa os nomes do NetBios no lugar dos endereços IP. Os dois executam ataques "man-in-the-middle". Esses ataques permitem que os agressores remotos leiam, insiram e modifiquem as mensagens trocadas entre dois pontos finais de comunicação sem serem notados. Os computadores expostos a tais ataques frequentemente param de responder ou reiniciam inesperadamente.

Para evitar ataques, recomendamos que você use senhas ou chaves de autenticação.

12.2.7 Ataques ICMP

O ICMP (Protocolo de Controle de Mensagens da Internet) é um protocolo de Internet popular e amplamente utilizado. Ele é utilizado primeiramente por computadores em rede para enviar várias mensagens de erro.

Os atacantes remotos tentam explorar a fraqueza do protocolo ICMP. O protocolo ICMP é destinado para a comunicação unidirecional que não requer qualquer autenticação. Isso permite que os atacantes remotos disparem ataques chamados de DoS (negação de serviço) ou ataques que dão acesso a pessoas não autorizadas aos pacotes de entrada e de saída.

Exemplos típicos de um ataque ICMP são ping flood, flood de ICMP_ECHO e ataques de smurfs. Os computadores expostos ao ataque ICMP são significativamente mais lentos (isso se aplica a todos os aplicativos que utilizam a Internet) e têm problemas para conectarem-se à Internet.

12.3 Email

Email ou correio eletrônico é uma forma moderna de comunicação e traz muitas vantagens. Ele é flexível, rápido e direto e teve papel crucial na proliferação da Internet no início dos anos 90.

Infelizmente, com os altos níveis de anonimato, o email e a Internet abrem espaço para atividades ilegais, como, por exemplo, spams. O spam inclui propagandas não solicitadas, hoaxes e proliferação de software malicioso – malware. A inconveniência e o perigo para você aumentam pelo fato de que o custo de enviar um spam é mínimo, e os autores do spam têm muitas ferramentas para adquirir novos endereços de email. Além disso, o volume e a variedade de spams dificultam muito o controle. Quanto mais você utiliza o seu email, maior é a possibilidade de acabar em um banco de dados de mecanismo de spam. Algumas dicas de prevenção:

- Se possível, não publique seu email na Internet,
- forneça seu email apenas a pessoas confiáveis,
- se possível, não use aliases comuns; com aliases mais complicados, a probabilidade de rastreamento é menor,
- não responda a spam que já chegou à sua caixa de entrada,

- tenha cuidado ao preencher formulários da Internet; tenha cuidado especial com opções, como *Sim, desejo receber informações*.
- use emails "especializados" - por exemplo, um para o trabalho, um para comunicação com amigos, etc.
- de vez em quando, altere o seu email,
- utilize uma solução antispam.

12.3.1 Anúncios

A propaganda na Internet é uma das formas de publicidade que mais cresce. As suas principais vantagens de marketing são custos mínimos e alto nível de objetividade; e o mais importante, as mensagens são enviadas quase imediatamente. Muitas empresas usam as ferramentas de marketing por email para se comunicar de forma eficaz com os seus clientes atuais e potenciais.

Esse tipo de publicidade é legítimo, desde que o usuário esteja interessado em receber informações comerciais sobre alguns produtos. Mas muitas empresas enviam mensagens comerciais em bloco não solicitadas. Nesses casos, a publicidade por email ultrapassa o razoável e se torna spam.

Hoje em dia a quantidade de emails não solicitados é um problema e não demonstra sinais de que vá diminuir. Os autores de emails não solicitados geralmente tentam disfarçar o spam enviando-o como mensagens legítimas.

12.3.2 Hoaxes

Hoax é a informação falsa disseminada pela Internet. Os hoaxes geralmente são enviados por email ou por ferramentas de comunicação, como ICQ e Skype. A própria mensagem geralmente é uma brincadeira ou uma lenda urbana.

Os hoaxes de vírus de computador tentam gerar FUD (medo, incerteza e dúvida) nos remetentes, levando-os a acreditar que há um "vírus desconhecido" excluindo arquivos e recuperando senhas ou executando alguma outra atividade perigosa em seu sistema.

Alguns hoaxes solicitam aos destinatários que encaminhem mensagens aos seus contatos, perpetuando-os. Há hoaxes de celular, pedidos de ajuda, pessoas oferecendo para enviar-lhe dinheiro do exterior etc. Na maioria dos casos, é impossível identificar a intenção do criador.

Se você receber uma mensagem solicitando que a encaminhe para todos os contatos que você conheça, ela pode ser muito bem um hoax. Há muitos sites especializados na Internet que podem verificar se o email é legítimo ou não. Antes de encaminhar, faça uma pesquisa na Internet sobre a mensagem que você suspeita que seja um hoax.

12.3.3 Phishing

O termo roubo de identidade define uma atividade criminosa que usa técnicas de engenharia social (manipulando os usuários a fim de obter informações confidenciais). Seu objetivo é obter acesso a dados confidenciais, como números de contas bancárias, códigos de PIN, etc.

O acesso geralmente é feito pelo envio de um email passando-se por uma pessoa ou negócio confiável (por exemplo, uma instituição financeira, empresa de seguros). O email pode parecer muito genuíno e conterá imagens e conteúdo que podem vir originalmente da fonte imitada. Você será solicitado a digitar, sob vários pretextos (verificação de dados, operações financeiras), alguns dos seus dados pessoais - número de conta bancária ou nomes de usuário e senhas. Todos esses dados, se enviados, podem ser facilmente roubados ou usados de forma indevida.

Bancos, companhias de seguros e outras empresas legítimas nunca solicitarão nomes de usuário e senhas em um email não solicitado.

12.3.4 Reconhecendo scams de spam

Geralmente, há poucos indicadores que podem ajudar a identificar spam (emails não solicitados) na sua caixa de correio. Se uma mensagem atender a pelo menos alguns dos critérios a seguir, muito provavelmente é uma mensagem de spam:

- O endereço do remetente não pertence a alguém da sua lista de contatos,
- você recebe uma oferta de grande soma de dinheiro, mas tem de fornecer primeiro uma pequena soma,
- você é solicitado a digitar, sob vários pretextos (verificação de dados, operações financeiras), alguns dos seus dados pessoais - número de conta bancária, nomes de usuário e senhas, etc.
- está escrito em um idioma estrangeiro,
- você é solicitado a comprar um produto no qual não tem interesse. Se decidir comprar de qualquer maneira, verifique se o remetente da mensagem é um fornecedor confiável (consulte o fabricante do produto original).
- algumas palavras estão com erros de ortografia na tentativa de enganar o filtro de spams. Por exemplo, *vaigra* em vez de *viagra*, etc.